

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341324

(43)Date of publication of application : 08.12.2000

(51)Int.Cl.

H04L 12/56

H04L 9/08

H04L 12/46

H04L 12/28

H04L 12/22

H04L 29/14

(21)Application number : 11-146948

(71)Applicant : NTT DATA CORP

(22)Date of filing : 26.05.1999

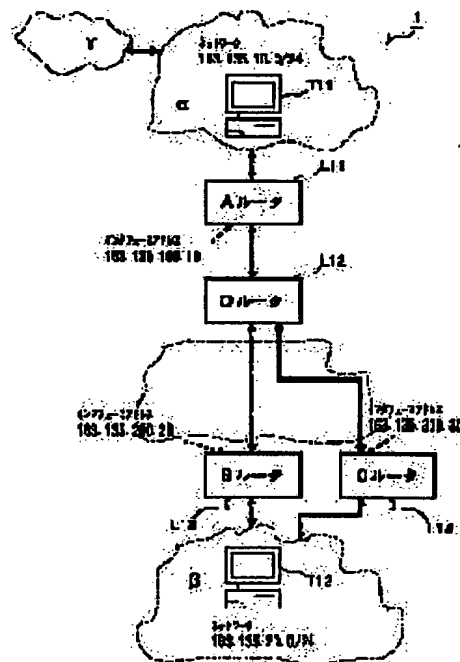
(72)Inventor : KUSAKA TAKAYOSHI
MATSUDA YOSHIYUKI
BABA TATSUYA

(54) CIPHER COMMUNICATION METHOD AND SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a cipher communication system that can continues cipher communication even when a decoder is changed due to a path change on the occurrence of a path fault during the cipher communication.

SOLUTION: Layout information relating to the layout of other routers L12 to L14 capable of cipher communication is included in path forming information of a router L11 that receives or transmits the path information such as a routing protocol. In the case that any router such as the router L13 on an optimum path during the cipher communication is disabled or communication, a new optimum path is formed again and continues the cipher communication with the other router L14 in existence on the optimum path formed again by using a key decided mutually.



LEGAL STATUS

[Date of request for examination] 09.12.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3821990

[Date of registration] 30.06.2006

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

MS002
31841

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-341324
(P2000-341324A)

(43)公開日 平成12年12月8日(2000.12.8)

| (51)Int.Cl. ⁷ | 識別記号 | F I | テマコード*(参考) |
|--------------------------|-------|---------------|-------------------|
| H 0 4 L | 12/56 | H 0 4 L 11/20 | 1 0 2 D 5 J 1 0 4 |
| | 9/08 | | 6 0 1 Z 5 K 0 3 0 |
| | 12/46 | | 3 1 0 C 5 K 0 3 3 |
| | 12/28 | | 5 K 0 3 5 |
| | 12/22 | | 3 1 1 9 A 0 0 1 |

審査請求 未請求 請求項の数10 O L (全 9 頁) 最終頁に続く

(21)出願番号 特願平11-146948
(22)出願日 平成11年5月26日(1999.5.26)

(71)出願人 000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(72)発明者 日下 貴義
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(72)発明者 松田 栄之
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(74)代理人 100099324
弁理士 鈴木 正剛

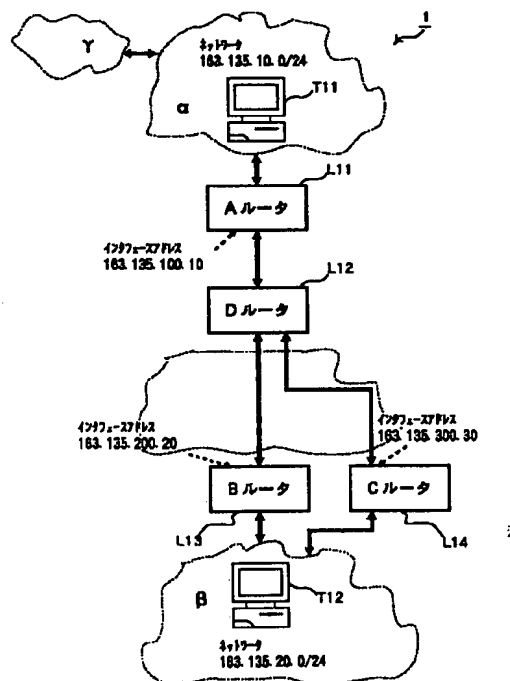
最終頁に続く

(54)【発明の名称】 暗号通信方法及びシステム

(57)【要約】

【課題】 暗号通信中に経路障害が発生し、経路変更に伴って復号化を行う装置が変わった場合にも暗号通信を継続できる暗号通信システムを実現する。

【解決手段】 ルーティングプロトコルのような経路形成情報の受け渡しを行うルータ L 1 1 の経路形成情報に、暗号通信可能な他のルータ L 1 2 ~ L 1 4 の配置に関する配置情報を含める。暗号通信中の最適経路上のいずれかのルータ、例えばルータ L 1 3 が通信不能になったときは、新たな最適経路を再形成するとともに、再形成された最適経路に存する他のルータ L 1 4 との間で相互に取り決めた鍵を用いて暗号通信を継続する。



【特許請求の範囲】

【請求項 1】 高可用通信と暗号通信とを同時に実現することができるネットワークを介して行う暗号通信方法であって、

前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことによりネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行うとともに、前記ネットワーク上における通信中継装置の構成が変更された場合に前記経路形成情報を更新して新たな最適経路を再形成し、再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続することを特徴とする、暗号通信方法。

【請求項 2】 各通信中継装置は、ある通信装置又はネットワークへ向かう暗号化された通信データの復号化ができる場合にその通信装置又はネットワークの識別情報を記録しておき、他の通信中継装置から前記経路形成情報を受け取ったときに暗号通信先が前記識別情報と同じ識別情報を保持していた場合に、前記他の通信中継装置との間で前記鍵の取り決めを行うことを特徴とする、請求項 1 記載の暗号通信方法。

【請求項 3】 所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことにより高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行う暗号通信システムであって、

各通信中継装置の経路形成情報は、前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、

前記複数の通信中継装置の少なくとも一つは、暗号通信中の最適経路上の通信中継装置の配置構成が変更になったことを検知したときに当該変更後の配置情報を他の通信中継装置に通知するように構成され、少なくとも他の一つは、前記通知をもとに自己の経路形成情報を更新して新たな最適経路を再形成するとともに再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続するように構成されていることを特徴とする、暗号通信システム。

【請求項 4】 所定の経路形成情報をもとに高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成するとともにこの最適経路に存在する他の通信中継装置との間で暗号通信を行う通信中継装置であって、

前記経路形成情報は、暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、

暗号通信中に前記最適経路における他の通信中継装置の

配置構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新する更新手段と、更新後の経路形成情報をもとに新たな最適経路を形成する経路形成手段と、

新たに形成された最適経路上の暗号通信可能な他の通信中継装置を検出する検出手段とを備え、当該検出した通信中継装置との間で取り決めた鍵を用いて暗号通信を継続することを特徴とする、通信中継装置。

【請求項 5】 前記経路形成情報が所定のルーティングプロトコルに基づいて他の通信中継装置との間で相互に受け渡しされる情報であって、暗号通信を行えるノードの配置に関する情報及びそのノードが暗号通信実施の対象とする通信経路の識別情報を含むものであり、前記識別情報に基づいて前記鍵を取り決めることを特徴とする、

請求項 4 記載の通信中継装置。

【請求項 6】 前記識別情報をもつノードとの間で取り決めた鍵を予め保持している場合はその鍵を索出し、鍵を保持していない場合は当該ノードとの間で鍵生成を行うことで前記鍵を確保することを特徴とする、

請求項 5 記載の通信中継装置。

【請求項 7】 前記更新手段は、暗号通信中に通信不能となった通信中継装置に関する配置情報を削除するように更新することを特徴とする、

請求項 4 記載の通信中継装置。

【請求項 8】 前記更新手段は、暗号通信中に増設された通信中継装置に関する配置情報を追加するように更新することを特徴とする、

請求項 4 記載の通信中継装置。

【請求項 9】 前記更新手段は、暗号通信中に移動された通信中継装置に関する配置情報を修正するように更新することを特徴とする、

請求項 4 記載の通信中継装置。

【請求項 10】 暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報をもとに、高可用通信と暗号通信とを同時に実現することができるネットワークネットワーク上における最適経路を形成する機能と、

通信相手装置との間で暗号通信を行う機能と、

前記通信相手装置の構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新し、更新後の経路形成情報をもとに新たな最適経路を形成するとともに、この新たな最適経路に存在する他の通信相手装置との間で取り決めた鍵を用いて暗号通信を継続する機能とをコンピュータ上に形成するためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、高可用通信（障害時でも経路切替による自動継続が可能な通信、つまり耐障害性をもつ通信、以下同じ）と暗号通信（暗号技術を利用した機密通信、以下同じ）とが同時に実現できるネットワークにおいて、暗号通信中に通信中継装置の構成の変更が生じ、最適経路が変化した場合であっても暗号通信を安全に継続できるようにするための暗号通信技術に関する。

【0002】

【従来の技術】IP（Internet Protocol）ネットワークを使用して行う暗号通信の形態は、従来より良く知られている。この種の暗号通信は、送信側の暗号化装置と受信側の復号化装置との間で生成した鍵（暗号鍵／復号鍵）を用いて行われる。この場合の通信の形態としては、エンド・ツー・エンドで暗号通信を行う形態と、通信経路上に通信データ、例えばパケットの暗号化及び復号化を行う通信装置（以下、「暗号装置」）を配置することによって暗号通信を行う形態とがある。

【0003】IPネットワークにおいて暗号通信に用いる鍵の生成、鍵交換、鍵設定の手順としては、例えばIKE（Internet Key Exchange：暗号鍵生成手順）方式等、様々な手法が存在する。送信側は、この生成された鍵（暗号鍵）を使用してIPパケットを暗号化し、受信側は、この鍵に対応した鍵（復号鍵）を用いてパケットを復号化する。

【0004】ところで、IPネットワークを使用して通信を行っている最中に最適経路に何らかの障害が発生した場合は、OSPF（Open Shortest Path First）等のルーティングプロトコルを使用したり、ルータ等の通信中継装置自身の持つバックアップ経路設定機能を使用したりして通信を回復させることができる。つまり、自動的に迂回経路を設定して通信を回復させることができる。以下、これらの通信回復方法の概要を説明する。

【0005】（1）ルーティングプロトコルを使用した場合

図6に示すように、通信装置T11と通信装置12との間のIPネットワーク上のノードにルータN11～N15が接続されているとする。正常時の最適経路は、通信装置T11→ルータN11→ルータN12→ルータN13→ルータN15→通信装置T12、あるいはその逆であり、各ルータN11～N15は、互いに持っている経路形成情報、すなわち各ルータが直接どのルータと通信可能か等を表す情報を交換し合い、ネットワーク間の最適経路を形成している。

【0006】この最適経路において、ルータN13に障害が発生した場合は、以下のような手順で通信の回復を行う。まず、ルータN13に隣接する正常なルータ、例えばルータN12が、ルーティングプロトコルの機能により、ルータN13に障害が発生したことを検知する。検知方法は、ルーティングプロトコルによって決められ

ている。障害を検知したルータN12は、「今までの経路が使用できなかったこと」や「リンクが無くなったこと」等の情報を、ルーティングプロトコルの機能により、隣接するルータN11、N14に通知する。これらの通知情報は、隣接するルータN15にもリレーされ、これによりルーティングドメイン（ルーティング情報を受け渡すルータのグループ）のすべてのルータに通知される。このように新しく通知される情報により、各ルータN11、N12、N14、N15が持つ経路形成情報は更新され、障害経路の代わりになる迂回経路、すなわち、通信装置T11→ルータN11→ルータN12→ルータN14→ルータN15→通信装置T12の経路が再形成される。

【0007】（2）バックアップ経路設定機能を使用した場合

図6に示した通信システムの中のあるルータ、例えばルータN12にバックアップ経路設定機能があり、ルータN12が中継経路に障害が発生したことを検知した場合（リンクの有無やポーリング（監視信号）、キープアライブ（回線がダウンしていないことを確かめるための信号）等による）、ルータN12は、バックアップ経路設定機能に基づいて、予め設定しておいた代替経路（バックアップ経路）に切り替えて通信を保つ。

【0008】

【発明が解決しようとしている課題】通常通信のみならず、暗号通信を行っている最中に最適経路に障害が発生した場合も、上記のルーティングプロトコルの機能やバックアップ経路設定機能を用いて迂回経路を形成することができる。しかしながら、暗号通信の場合は、ルーティングプロトコルの機能あるいはバックアップ経路への切替機能と暗号通信の機能とが別構成になっているため、既存の仕組みのままでは、暗号化されたIPパケット（暗号化データ）を復号化することができず、暗号通信を継続できない場合がある。このことを以下に説明する。

【0009】ここでは、図7に示す構成、すなわち、ルータN12に暗号装置M21を介して通信装置T11が接続され、ルータN15に通信装置T22が接続され、さらにルータN12とルータN15との間に、それぞれ暗号装置M22、M23が並列に接続されたIPネットワーク構成を想定する。

【0010】各ルータN12、N15及び暗号装置M21、M22は、互いに持っている経路形成情報を交換しあい、ネットワーク間の最適経路を形成している。正常時における最適経路、つまり通常経路で収束した場合の経路は、通信装置T11→暗号装置M21→ルータN12→暗号装置M22→ルータN15→通信装置T12であり、暗号装置M21は、通信装置T22から送信されるパケットを、自装置と暗号装置M22との間で用いられる鍵（例えば鍵A）を用いて暗号化する。

10

20

30

40

50

【0011】この状態で、暗号装置M22で何らかの障害が発生し、ルーティングプロトコルの機能により経路変更が行われ、最適経路が通信装置T11→暗号装置M21→ルータN12→暗号装置M23→ルータN15→通信装置T12に自動的に変更されたとする。この場合、暗号装置M21と暗号装置M23との間で用いられる鍵（例えば鍵B）は、前述した鍵Aとは異なっている。しかし、暗号装置M21では、パケットの送信先（通信装置T12）に変更がないので、通信装置T11から通信装置T12宛に送信されるデータの暗号用鍵を鍵Aから鍵Bに変更すべきであることを従来のルーティングプロトコルからは認識することができない。そのため、当該パケットは暗号装置M21で鍵Aで暗号化されることになり、鍵Bを用いる暗号装置M23ではこれを復号することができないので、結局、暗号通信を回復することができない。

【0012】暗号通信には、送信先のアドレスを含むIPヘッダとパケットのデータ部分（すなわちペイロード）をまとめて暗号化し、新たな送信先（復号化装置）のアドレスを含むIPヘッダを付して通信を行うトンネルモードと、送信先アドレスは暗号化せず、パケットのデータ部分だけを暗号化するトランスポートモードとがあるが、いずれのモードでも、上記のように暗号装置M22で障害が発生したときに、暗号装置M21では鍵の変更の必要性を認識することができない。

【0013】このような問題は、暗号通信中に経路障害が発生した場合のみならず、それまで最適経路であった箇所（ノード）に、新たにルータ、暗号装置、通信装置等が増設された場合や、ルータ等の一部が移動した場合においても共通に生じる。これは、従来のこの種の高可用通信におけるルータ等の配置が固定的であり、暗号通信に用いられる鍵も固定的であったことに起因する。

【0014】そこで本発明は、高可用通信と暗号通信とが同時に実現できるネットワークにおいて、暗号化及び復号化を行う装置の配置構成に変更が生じた場合であっても、暗号用の鍵を動的に変更して暗号通信を安全に継続できるようにする技術を提供することを主たる課題とする。

【0015】

【課題を解決するための手段】上記課題を解決ため、本発明は、改良された暗号通信方法、暗号通信システム、通信中継装置、及び通信中継装置をコンピュータにより実現する上で好適となる記録媒体を提供する。

【0016】本発明の暗号通信方法は、高可用通信と暗号通信とを同時に実現することができるネットワークを介して行う方法であって、ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことによりネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信デー

タの暗号通信を行うとともに、前記ネットワーク上における通信中継装置の構成が変更された場合に前記経路形成情報を更新して新たな最適経路を再形成し、再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続することを特徴とする。各通信中継装置は、ある通信装置又はネットワークへ向かう暗号化された通信データの復号化ができる場合にその通信装置又はネットワークの識別情報を記録しておき、他の通信中継装置から経路形成情報を受け取ったときに暗号通信先が前記識別情報と同じ識別情報を保持していた場合に、前記他の通信中継装置との間で鍵の取り決めを行うようにする。

【0017】本発明の暗号通信システムは、所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことにより高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行う暗号通信システムである。各通信中継装置の経路形成情報は、前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、複数の通信中継装置の少なくとも一つは、暗号通信中の最適経路上の通信中継装置の配置構成が変更になったことを検知したときに当該変更後の配置情報を他の通信中継装置に通知するように構成され、少なくとも他の一つは、前記通知をもとに自己の経路形成情報を更新して新たな最適経路を再形成するとともに再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続するように構成されていることを特徴とする。

【0018】本発明の通信中継装置は、所定の経路形成情報をもとにネットワーク上における通信データの最適経路を形成するとともにこの最適経路に存在する他の通信中継装置との間で暗号通信を行う通信中継装置において、前記経路形成情報は、暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、暗号通信中に通信相手となる他の通信中継装置が通信不能になったときに自己の経路形成情報に含まれる前記配置情報の内容を更新する手段と、更新後の経路形成情報をもとに新たな最適経路を形成する手段と、新たに形成された最適経路上の暗号通信可能な他の通信中継装置を検出する手段とを備え、当該検出した通信中継装置との間で取り決めた鍵を用いて暗号通信を継続することを特徴とする装置である。

【0019】経路形成情報は、より具体的には所定のルーティングプロトコルに基づいて他の通信中継装置との間で相互に受け渡しされる情報であって、暗号通信を行えるノードの配置に関する情報及びそのノードが暗号通信実施の対象とする通信経路の識別情報を含むものであり、この識別情報に基づいて前記鍵を取り決めるようにする。識別情報をもつノードとの間で取り決めた鍵を予

め保持している場合はその鍵を索出し、鍵を保持していない場合は当該ノードとの間で鍵生成を行うことで前記鍵を確保するようにする。

【0020】通信中継装置における更新手段は、暗号通信中に通信不能となった通信中継装置がある場合はそれに関する配置情報を削除し、暗号通信中に増設された通信中継装置がある場合はそれに関する配置情報を追加し、暗号通信中に移動された通信中継装置がある場合はそれに関する配置情報を修正する。

【0021】本発明が提供する記録媒体は、暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報をもとに、高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成する機能と、通信相手装置との間で暗号通信を行う機能と、前記通信相手装置の構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新し、更新後の経路形成情報をもとに新たな最適経路を形成するとともに、この新たな最適経路に存在する他の通信相手装置との間で取り決めた鍵を用いて暗号通信を継続する機能とをコンピュータ上に形成するためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体である。

【0022】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。本発明では、高可用通信と暗号通信とが同時に実現できるネットワークにおいて、ルーティングプロトコルに従って経路形成情報の受け渡しを行う装置間で暗号通信を行っている場合に、暗号通信が可能な装置の配置に関する情報を上記経路形成情報に含め、経路形成情報と鍵の変更にに関する情報とをリンクさせるようにする。例えば、リンクステート式のルーティングプロトコルであれば、どのリンクに暗号通信可能な装置が配置されていてどのネットワーク間で暗号通信を行えるのか、ディスタンスベクトル式のルーティングプロトコルであれば、その距離ベクトル中にどのルータが存在するかを、経路形成情報の中に含める。そして、暗号化データを送信する際に、受信先の暗号装置に対応した鍵を用い、対応した鍵が無ければ新たに生成する、ということを経路形成情報に含める。なお、鍵の使用・生成は、従来から一般的に用いられていた手法を利用することができる。

【0023】上述の暗号通信方法は、例えば図1に示すように構成される暗号通信システムによって実施することができる。この暗号通信システム1は、 α ネットワーク上に配された送信側の通信装置T11、 β ネットワーク上に配された受信側の通信装置T12、これらの通信装置間に介在する複数のルータ、すなわちAルータL11、DルータL12、BルータL13、CルータL14その他のネットワーク構成部品を含み、高可用通信と暗号通信とを同時に実現できるように構成される。 α ネッ

トワークと β ネットワークとはインターネットのような広域通信網を介して接続されているものとする。

【0024】各ルータL11～L14は、メモリ及びCPUを有する一種のコンピュータであり、そのCPUが所定の記録媒体に記録されたプログラムコードを読み込んで実行されることによって形成されるルーティングプロトコルの機能、暗号通信の機能、及び、これらの機能を連携させる機能を有する。このプログラムコードを記録した記録媒体は、ルータに実装されるときには、例えばCPUが読みとり可能な半導体メモリ等の固定型記録媒体であるが、CD-ROM等の可搬性記録媒体を通じて流通し、実装時に上記固定型記録媒体にインストールされるものであっても良い。ルーティングプロトコルの機能については、従来のルータのものと基本的には同じであるが、ルーティングプロトコルで他のルータと交換する経路形成情報に次の二つの情報を含め、暗号通信の機能を連携させるようにした点で従来のルータが備える機能と異なる。

(1) 暗号通信を行えるノード(ルータ)の配置やインタフェースID

例:「暗号通信ができるAノードにAルータがある」

(2) そのノードが暗号通信実施の対象とする通信経路ID

例:「Aルータにおける暗号通信の対象(通信経路ID)は、 α ネットワーク及び β ネットワークの通信に対するものである」

これらの情報に対応するデータの形式は、適応するネットワークプロトコルやルーティングプロトコルに合わせたものになる。例えばIPネットワークのOSPFの場合は、後述するLSA(Link State Advertisement)にその情報を含めることになる。

【0025】一方、暗号通信の機能に関して、各ルータは、以下のようにして暗号通信を行う。

(1) 暗号通信実施対象の通信経路IDに対応する通信に対して、通信データ、例えばパケットを暗号化し、暗号化データを生成する。

例:「Aルータを通過するパケットのソースアドレスが β ネットワークに属し、ディスティネーションアドレスが β ネットワークに属するパケットは、ディスティネーションアドレスが通信経路IDに適合するので、暗号通信の対象とする」

(2) 暗号用の鍵は、通信経路に対応する通信経路IDを持ったノードのものを予め保持している場合はそれを索出して使用する。鍵を保持していない場合は、そのノード(ルータ)との間で鍵生成を行うことで、鍵を確保する。

例:「Aルータから β ネットワーク宛の経路上に、Bルータという暗号通信が可能なルータが存在し、そのBルータが β ネットワークに対して暗号通信実施の対象としていることを、ルーティングプロトコルによりAルータ

は知っている。そこで、暗号通信の対象となったパケットをBルータに対応する鍵を使用して暗号化する」両者の機能をリンクさせる機能については後述する。

【0026】なお、以上の機能は、全てのルータL11～L14が備えていることが望ましいが、通信装置T11から送られたパケットを暗号化して中継するいずれか中心的に作用するルータのみが備えている場合であっても本発明の実施は可能である。

【0027】次に、本実施形態の暗号通信システム1による通信形態を説明する。ここでは、図示のように、αネットワーク内の通信装置T11とAルータL11間のネットワークアドレスが「163.135.10.0/24」、βネットワーク内の通信装置T12とBルータL13又はCルータL14との間のインタフェースアドレスが「163.135.20.0/24」、AルータL11のインタフェースアドレスが「163.135.100.10」、BルータL13のインタフェースアドレスが「163.135.200.20」、CルータL14のネットワークアドレスが「163.135.300.30」であるものとし、リンクステート式ルーティングプロトコルの代表である上記OSPFの改良を行って暗号通信を行う場合の例を挙げる。OSPFについては、国際機関IETFで発行している仕様RFC2328、RFC1131、STD0054に詳細に記載されている。

【0028】OSPFで使用される経路形成情報、すなわちリンク状態広告パケット(LSA: Link State Advertisement)のうち、各ルータL11～L14が送信するルータリンクLSAのフォーマット例を図2に示す。このルータリンクLSAは、隣接ルータ間で受け渡される各種リンク情報であり、リンク状態ヘッダとLSA部とから構成される。LSA部には、ルータタイプ、リンクID、リンクデータ等が記述されており、これに記述される情報によって各ルータが他のルータの配置に関する情報を認識でき、経路計算、又は再計算に利用することができるようになる。図3は、ルータタイプの内容と、それに対するリンクID、リンクデータの例とを示したものである。タイプ1～4は、既存のルータが具備する情報であり、タイプ5が、本実施形態で追加した部分、つまり、暗号通信に関連する情報である。このタイプ5の記述によって、どのルータがどこで暗号通信を行っているかをわかるようにする。タイプ5において、リンクデータがNullの場合は、まだ決定されていないどこかと暗号通信ができることを示す。

【0029】LSAは、各ルータL11～L14で持てるリンク情報を複数発信することができる。従って、一つのルータが複数のルータとの間で暗号通信を行っていれば、暗号通信用LSAも複数指定できる。例えば、タイプ5のLSAでリンクIDが「163.135.100.10」、リンクデータが「163.135.20.0/24」であれば、このLSAを送信した「163.135.100.10」をアドレスとして持つルータは、「163.135.20.0/24」というアドレスを持つ

相手先と暗号通信ができる状態であることを示す。さらに、リンクIDまで同じで、リンクデータ「163.135.30.0/24」のLSAがあれば、ルータ「163.135.100.10」は、「163.135.30.0/24」の相手先とも暗号通信ができる状態であることを示す。

【0030】このような改良OSPFを使用し、パケットを暗号化して送信する場合、各ルータL11～L14は、暗号通信先の情報をLSAで宣言することになる。この宣言には、暗号通信元の情報も含まれる。各ルータL11～L14は、また、あるネットワークへ向かうパケットの復号化ができる場合、ルータ自身のデータベースにそのネットワークの情報を「暗号通信受け持ちネットワーク(又はホスト)」として記録する。この情報は、各ルータが、他のルータの暗号通信LSAを受け取ったときにその暗号通信先と同じ「暗号通信受け持ちネットワーク」を持っていた場合に、そのLSA送信元ルータとの間で鍵生成を行うために必要な情報となる。

【0031】ルータ同士は、それぞれHelloパケット(隣接ルータに対するキープアライブ信号のようなもの)の受け渡しを行っており、この受け渡しが可能なルータ間では、それぞれ自己のLSAがリンクバイリンクで相手側に伝わるようになっている。例えば、BルータL13及びCルータL14が暗号化及び復号化が可能なルータである場合は、その旨及びそれが正常に動作していることが、DルータL12を通じてAルータL11に伝わる。AルータL11は、BルータL13のLSAにより、そのルータL13が自己の「暗号通信受け持ちネットワーク」と暗号通信を行う用意があることを知り、BルータL13との間で暗号用の鍵を生成するプロセスを実施する。このプロセスは、一般に用いられている鍵生成のプロセスであって構わない。AルータL11は、また、CルータL14との間でも鍵を生成するプロセスを実施する。

【0032】図4(a)は、通常経路で収束したときのAルータL11のリンクテーブル(ルーティングテーブルの元情報)の内容を示した図である。図示の例では、AルータL11は、αネットワーク及びDルータL12とリンクしており、暗号通信受け持ちネットワークはαとγである。BルータL13、CルータL14は、βネットワークとDルータL12とリンクしており、「暗号通信受け持ちネットワーク」は共にβである。Dルータは、AルータL11、BルータL13、CルータL14とリンクしており、「暗号通信受け持ちネットワーク」の指定がない又は未だ決定されていないどこかである。なお、「暗号通信受け持ちネットワーク」は、必ずしも隣接している必要はない。

【0033】このリンクテーブルから、AルータL11は、ネットワークαからネットワークβへの最適経路を、αネットワーク(通信装置T11)→AルータL11→DルータL12→BルータL13→βネットワーク

(通信装置 T12) のように形成する。

【0034】一方、A ルータ L11 は、図 4 (a) のリンクテーブルと連携して暗号化フィルタを図 5 (a) のように設定する。すなわち、A ルータ L11 の「暗号通信受け持ちネットワーク」は α ネットワークであり、経路上に β を「暗号通信受け持ちネットワーク」とするルータは B ルータ L13 である。そこで、A ルータ L11 は、B ルータ L13 との間で鍵 a の生成を行う (鍵 a を既に保持してある場合は、それを索出する)。このリンクテーブルの意味は、「発信元アドレス (ネットワーク) が α で、送信先アドレス (ネットワーク) が β のパケット ($\alpha \rightarrow \beta$) を、鍵 a で暗号化して B ルータ L13 へ送信 (set peer(B)) せよ」である。これにより鍵 a を用いた暗号通信が可能になる。

【0035】ここで、B ルータ L13 に障害が発生した場合を考える。この場合は、B ルータ L13 が発する LSA が D ルータ L12 及び A ルータ L11 に届かないため、A ルータ L11 は、ルーティングプロトコルの機能を用いて B ルータ L13 が使えないものとして経路を回復させる。図 4 (b) は、回復経路で収束したときの A ルータ L11 のリンクテーブル (ルーティングテーブルの元) の更新後の内容を示した図である。図示のように、B ルータ L13 のリンク情報が無くなっている。このリンクテーブルから、最適経路は、 α ネットワーク (通信装置 T11) \rightarrow A ルータ L11 \rightarrow D ルータ L12 \rightarrow C ルータ L14 $\rightarrow \beta$ ネットワーク (通信装置 T12) のように変更されるが、本実施形態では更に、経路変更と連携して A ルータ L11 が使用する鍵 a を鍵 c に動的に変更させる。

【0036】すなわち、A ルータ L11 は、図 4 (b) のリンクテーブルが更新されると、これに連携して暗号化フィルタの内容を図 5 (b) のように更新する。すなわち、経路上に β を「暗号通信受け持ちネットワーク」とするルータは C ルータ L14 であることがわかるので、A ルータ L11 は、C ルータ L14 との間で鍵 c の生成を行う (鍵 c を既に保持してある場合は、それを索出する)。このリンクテーブルの意味は、「発信元アドレス (ネットワーク) が α で、送信先アドレス (ネットワーク) が β のパケット ($\alpha \rightarrow \beta$) を、鍵 c で暗号化して C ルータ L14 へ送信 (set peer(B)) せよ」である。

【0037】このように、B ルータ L13 に障害が発生し、経路変更がなされても、更新後のルーティングプロトコルによるリンクテーブルから図 5 (b) のような暗号化フィルタの設定が得られ、経路変更に伴う鍵の変更がなされるので、暗号通信を継続できるようになる。

【0038】なお、本実施形態では、暗号通信可能なルータの配置構成に変更が生じ、これによって使用する鍵が変更される場合の例として、ルータの故障等による経路障害が生じたことを想定したが、本発明は、このよう

な例のみではなく、例えばネットワーク上にルータを増設し、あるいはあるネットワークから他のネットワークにルータを移動させた結果、使用する鍵が変更される場合にも同様に適用が可能である。すなわち、手動による暗号通信の設定を行うことなく、ルーティングプロトコルの機能を用いて相互に経路形成情報を受け渡し、その配置情報を各ルータで更新し、最適経路を自動的に形成することで、暗号通信を継続することが可能である。また、ルータの経路形成情報に、暗号通信を行う対象のネットワークないしホストを指定するだけで、当該ルータが自動的に暗号通信を行う相手先装置を見つけ出すことも可能となる。これらの機能は、あるネットワーク上に接続されるルータの数が絶えず増減するという現実の通信形態に即した機能であり、これによってモバイル型通信の普及にも容易に対応が可能になるものである。

【0039】本実施形態では、通信中継装置としてルータを例に挙げて説明したが、本発明の仕組みは、暗号通信の相手先が変化する場合のある装置全般に適用することが可能である。また、本実施形態のように経路形成情報を他の装置と相互に受け渡す機能と暗号用の鍵を動的に変更させる機能とを一つの装置 (例えばルータ) 内に設けることは好ましい形態であるが、常にこのような形態にしなければならないというものではない。例えばルータに接続された通信装置が、ルータからの通知に基づいて暗号用の鍵を動的に変更する機能をもつように構成することは、本発明の暗号通信方法を実施する上で支障とはならない。

【0040】本実施形態では、IP ネットワークを通信媒体とした例について説明したが、本発明は、高可用通信と暗号通信とを同時に実現することができるネットワークであれば、その規模にかかわらず適用が可能なので、アンセキュアなネットワークであるイントラネットやエクストラネットでの利用も可能である。

【0041】本発明の適用には、ルーティングプロトコルのような経路形成情報の相互受け渡し機能が前提となるため、他の独自のルーティングプロトコルを使っていたり、ルーティングプロトコルの相互接続ができない ISP (Internet Service Provider) を利用する場合は、その ISP を利用しない閉域網内で利用することになるが、その ISP を利用した場合であっても、経路形成情報を公知のトンネリング技術で ISP のサービスによらない方法で中継することにより、閉域網を越えたネットワークでの利用も可能である。

【0042】本発明は、暗号通信先が物理的もしくは論理的に頻繁に変更になる場合に特に有効であり、モバイルネットワークといった網構成変更にも柔軟に対応が可能である。

【0043】本発明は、また、コンシューマ用暗号通信市場 (個人を対象としたネットワークサービスの利用の一形態) への適用も可能である。現在、個人を対象とし

た暗号通信技術の主流は SSL (Secure Socket Layer) である。これは、通信の上位層で暗号化するもので、個人が操作する端末（通信装置）自らが通信データを暗号化して送信することによりエンド・ツー・エンドの暗号通信を行うことを目的とする。本発明をこの個人が操作する端末（モバイル型端末を含む）がアクセスするネットワークに適用させることは、上記ネットワークサービスを促進する上で有効な手段となり得る。

【0044】

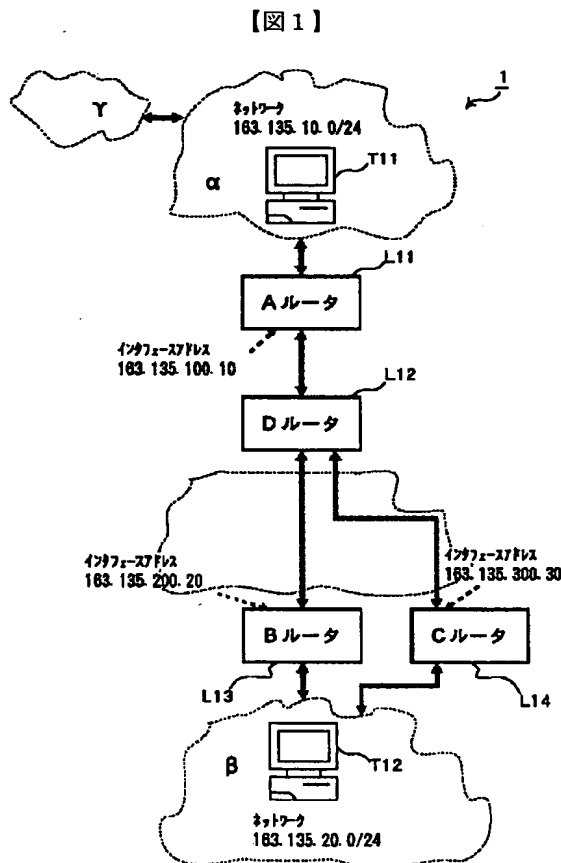
【発明の効果】以上の説明から明らかなように、本発明によれば、暗号通信中に経路変更が行われた結果、復号化する装置、つまり鍵に変更が生じた場合であっても、暗号通信を安全且つ確実に継続できるようになるという、特有の効果がある。

【図面の簡単な説明】

【図1】本発明を適用した暗号通信システムの構成図。

【図2】ルータリンク LSA のフォーマット例を示した図。

【図3】ルータリンク LSA のタイプ種類を示した図。*



* 【図4】(a)は、ルーティングプロトコルを用いた場合の最適経路を形成する場合に使用されるリンクテーブルの内容説明図、(b)は障害発生時に更新されるリンクテーブルの内容説明図。

【図5】(a)は、正常動作時における暗号化フィルタの設定内容を示した図、(b)は障害発生時に更新される暗号化フィルタの設定内容を示した図。

【図6】従来における、ルーティングプロトコルを用いた場合の最適経路復旧の説明に用いるためのネットワーク構成図。

【図7】従来における、ルーティングプロトコル及び暗号通信を用いた場合の最適経路復旧の説明に用いるためのネットワーク構成図である。

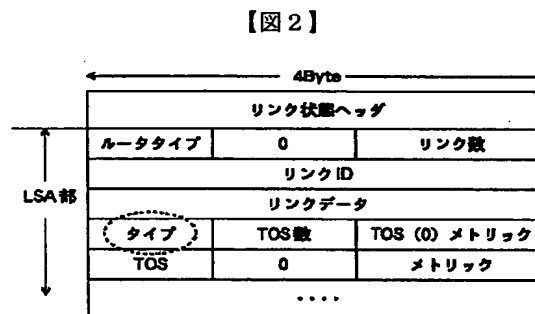
【符号の説明】

1 暗号通信システム

T11, T12 通信装置

L11~L14, N11~N15 ルータ

M21~M23 暗号装置



【図3】

| タイプ | 内容 | リンクID | リンクデータ |
|------------|-----------|--|----------------------------------|
| 1 | 他ルータへのリンク | 隣接ルータのルータID | インタフェース番号 (またはIPアドレス) |
| 2 | 通過ネットワーク | 代表ルータへのアドレス | ルータのそのネットワーク上のIPアドレス |
| 3 | サブネットワーク | ネットワークアドレス、ネットワークマスク | プレフィックス長 |
| 4 | 仮想リンク | 隣接ルータのルータID | ルータのそのネットワーク上のIPアドレス |
| 5 (追加する部分) | 暗号通信 | 暗号通信ができる自ルータのIPアドレスかルータID、またはインタフェース番号、またはインタフェースのIPアドレス | 暗号通信ができる相手先のネットワークアドレスまたはホストアドレス |

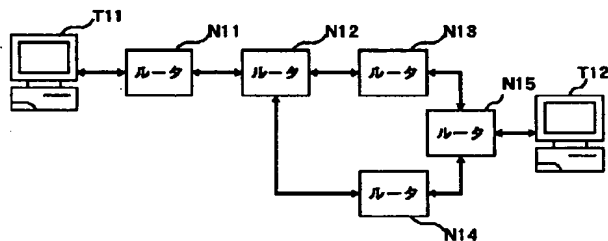
【図 4】

| ルータ | A | B | C | D |
|--------------------|-----------------------|----------------------|----------------------|-------------------------|
| 持っているリンク (コスト) | α (1) D (1) | β (1) D (1) | β (1) D (2) | A (1) B (1) C (2) |
| 暗号通信受け持ち ネットワーク | α Y | β | β | N/A |

(b)

| ルータ | A | C | D |
|--------------------|-----------------------|----------------------|-------------------------|
| 持っているリンク (コスト) | α (1) D (1) | β (1) D (2) | A (1) B (1) C (2) |
| 暗号通信受け持ち ネットワーク | α Y | β | N/A |

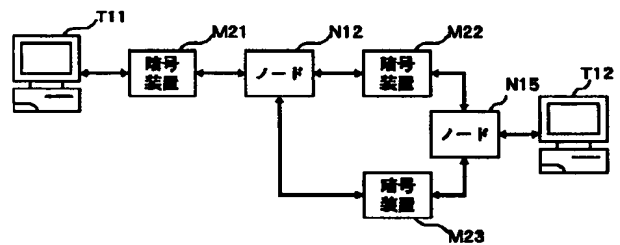
【図 6】



【図 5】

| (a) | (b) |
|----------------------------------|----------------------------------|
| match $\alpha \rightarrow \beta$ | match $\alpha \rightarrow \beta$ |
| set peer (B) | set peer (C) |
| key a | key c |

【図 7】



フロントページの続き

(51) Int. Cl.⁷

H04L 29/14

識別記号

F I

テーマコード (参考)

(72) 発明者 馬場 達也

東京都江東区豊洲三丁目 3 番 3 号 株式会
社エヌ・ティ・ティ・データ内F ターム (参考) 5J104 AA01 AA34 BA02 NA02 NA37
PA07

5K030 GA12 GA15 HD03 KA05 LB05

5K033 AA06 AA08 CB08 DA05 DB18
EC03

5K035 CC09 DD01 LL17

9A001 BB02 BB04 CC06 CC07 DD10

EE03 HH09 JJ18 LL07 LL09

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

(57) [Claim(s)]

[Claim 1]

It is the cryptocommunication approach of performing communication link for Takayoshi, and cryptocommunication through a network realizable to coincidence,

The optimal path on a network is formed by exchanging mutually predetermined path formation information including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible among two or more communication link repeating installation, and suiting on said network. While performing cryptocommunication of commo data between the communication link repeating installation which exists in this optimal path When the configuration of the communication link repeating installation on said network is changed, said path formation information is updated and it is characterized by continuing said cryptocommunication using the key fixed mutually between the communication link repeating installation which carries out the reconstitution of the new optimal path, and consists in the optimal path by which the reconstitution was carried out and in which cryptocommunication is possible, The cryptocommunication approach.

[Claim 2]

Each communication link repeating installation records the identification information of the communication device or a network, when a decryption of the enciphered commo data which goes to a certain communication device or network can be performed, and when said path formation information is received from other communication link repeating installation and the cryptocommunication point holds the same identification information as said identification information, it is characterized by settling on said key between communication link repeating installation besides the above, The cryptocommunication approach according to claim 1.

[Claim 3]

It is the cryptocommunication system which performs cryptocommunication of commo data between the communication link repeating installation which forms the optimal path on the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence, and exists in this optimal path by exchanging predetermined path formation information mutually among two or more communication link repeating installation, and suiting,

The path formation information on each communication link repeating installation includes the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible on said network,

At least one of said two or more of the communication link repeating installation It is constituted so that the arrangement information after the modification concerned may be notified to other communication link repeating installation, when it detects that the arrangement configuration of the communication link repeating installation on the optimal path under cryptocommunication was changed. Other one [at least] While updating the path formation information on self based on said notice and carrying out the reconstitution of the new optimal path to it, it is characterized by being constituted so that said

cryptocommunication may be continued using the key fixed mutually between the communication link repeating installation which consists in the optimal path by which the reconstitution was carried out and in which cryptocommunication is possible,
Cryptocommunication system.

[Claim 4]

While forming the optimal path on the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence based on predetermined path formation information, it is the communication link repeating installation which performs cryptocommunication among other communication link repeating installation which exists in this optimal path,

Said path formation information includes the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible,

An updating means to update the contents of said arrangement information included in the path formation information on self when the arrangement configuration of other communication link repeating installation in said optimal path is changed during cryptocommunication,

Path means forming which forms a new optimal path based on the path formation information after updating,

It has a detection means to detect other communication link repeating installation in which the cryptocommunication on the newly formed optimal path is possible,

It is characterized by continuing cryptocommunication using the key fixed between the detected communication link repeating installation concerned,

Communication link repeating installation.

[Claim 5]

it is the information by which said path formation information is mutually delivered and carried out among other communication link repeating installation based on a predetermined routing protocol, and the information about arrangement of the node which can perform cryptocommunication, and its node are characterized by fixing said key based on said identification information including the identification information of the communication path made into the object of cryptocommunication implementation
Communication link repeating installation according to claim 4.

[Claim 6]

When the key fixed between nodes with said identification information is held beforehand, the key is ****(ed), and when the key is not held, it is characterized by securing said key by performing key generation between the nodes concerned,

Communication link repeating installation according to claim 5.

[Claim 7]

It is characterized by updating said updating means so that the arrangement information about the communication link repeating installation used as communication link impossible may be deleted during cryptocommunication,

Communication link repeating installation according to claim 4.

[Claim 8]

It is characterized by updating said updating means so that the arrangement information about the communication link repeating installation extended during cryptocommunication may be added,

Communication link repeating installation according to claim 4.

[Claim 9]

It is characterized by updating said updating means so that the arrangement information about the communication link repeating installation moved during cryptocommunication may be corrected,

Communication link repeating installation according to claim 4.

[Claim 10]

The function which forms the optimal path on the network network which can realize communication link for Takayoshi, and cryptocommunication to coincidence based on predetermined path formation information including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible,

The function to perform cryptocommunication between communications-partner equipment,
The record medium with which the program code for forming on a computer the function which
continues cryptocommunication using the key which fixed among other communications-partner
equipments which exist in this new optimal path while update the contents of said arrangement
information included in the path formation information on self and forming a new optimal path based on
the path formation information after updating, when the configuration of said communications-partner
equipment is changed was recorded and in which a computer readout is possible.

[Translation done.]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention]

Modification of the configuration of communication link repeating installation arises during cryptocommunication, and even if this invention is the case where an optimal path changes, it relates to the cryptocommunication technique for continuing cryptocommunication safely in the network which the communication link for Takayoshi (it is the same the communication link which has the communication link in which the automatic continuation by path change is possible, i.e., failure-proof nature, also in the time of a failure, and the following), and cryptocommunication (it is the same the secret communication link using a code technique and the following) can realize to coincidence.

[0002]

[Translation done.]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art]

The gestalt of the cryptocommunication performed using IP (Internet Protocol) network is known better than before. This kind of cryptocommunication is performed using the key (a cryptographic key / decode key) generated between the encryption equipment of a transmitting side, and the decryption equipment of a receiving side. As a gestalt of the communication link in this case, there are a gestalt which performs cryptocommunication by end to end, and a gestalt which performs cryptocommunication by arranging the communication device (following, "data encryption equipment") which performs encryption and a decryption of commo data, for example, a packet, on a communication path.

[0003]

As a procedure of generation of the key used for cryptocommunication in IP network, key exchange, and a key setup, various technique, such as an IKE (Internet Key Exchange: cryptographic key generation procedure) method, exists, for example. A transmitting side enciphers an IP packet using this generated key (cryptographic key), and a receiving side decrypts a packet using the key (decode key) corresponding to this key.

[0004]

By the way, when a certain failure occurs at an optimal path in the midst which is communicating using IP network, a communication link can be recovered, and using the backup routing function which the communication link repeating installation itself, such as a router, has. [using routing protocols such as OSPF (Open Shortest Path First),] That is, an alternate route can be set up automatically and a communication link can be recovered. Hereafter, the outline of these communication link methods of recovery is explained.

[0005]

(1) When a routing protocol is used

As shown in drawing 6, suppose that routers N11-N15 are connected to the node on IP network between a communication device T11 and a communication device 12. The optimal path of forward always exchanges mutually the information [information / , i.e., express which router and communication link are directly possible for each router, / the communication device T11 -> router N11 -> router N12 -> router N13 -> router N15 -> communication device T12 or its path formation information / information / which is reverse and has mutually each routers N11-N15], and forms the optimal path between networks.

[0006]

In this optimal path, when a failure occurs in a router N13, the following procedures recover a communication link.

First, the normal router N12 which carries out proximal to a router N13, for example, a router, detects that the failure occurred in the router N13 by the function of a routing protocol. The detection approach is determined by the routing protocol. The router N12 which detected the failure notifies information, such as "an old path was not able to be used" or "the link having been lost", to the adjoining routers N11 and N14 by the function of a routing protocol. Such notice information is relayed also to the adjoining

router N15, and, thereby, is notified to all the routers of a routing domain (group of a router who delivers routing information). Thus, the path formation information which each routers N11, N12, N14, and N15 have is updated by the information notified newly, and the reconstitution of the alternate route which becomes instead of a failure path, i.e., the path of the communication device T11 -> router N11 -> router N12 -> router N14 -> router N15 -> communication device T12, is carried out.

[0007]

(2) When a backup routing function is used

A backup routing function is in a certain router N12 in the communication system shown in drawing 6, for example, a router. the case (polling (supervisory signal) the existence of a link --) where a router N12 detects that the failure occurred for the junction path it is based on keep alive (signal for confirming that the circuit is not downed) etc. -- a router N12 is changed to the alternate route (backup path) set up beforehand based on a backup routing function, and maintains a communication link.

[0008]

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention]

Even if it is the case where modification arises to the equipment to decrypt, i.e., a key, as a result of making a path change during cryptocommunication according to this invention so that clearly from the above explanation, there are insurance and characteristic effectiveness [say / that it can continue now certainly] about cryptocommunication.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

Modification of the configuration of communication link repeating installation arises during cryptocommunication, and even if this invention is the case where an optimal path changes, it relates to the cryptocommunication technique for continuing cryptocommunication safely in the network which the communication link for Takayoshi (it is the same the communication link which has the communication link in which the automatic continuation by path change is possible, i.e., failure-proof nature, also in the time of a failure, and the following), and cryptocommunication (it is the same the secret communication link using a code technique and the following) can realize to coincidence.

[0002]

[Description of the Prior Art]

The gestalt of the cryptocommunication performed using IP (Internet Protocol) network is known better than before. This kind of cryptocommunication is performed using the key (a cryptographic key / decode key) generated between the encryption equipment of a transmitting side, and the decryption equipment of a receiving side. As a gestalt of the communication link in this case, there are a gestalt which performs cryptocommunication by end to end, and a gestalt which performs cryptocommunication by arranging the communication device (following, "data encryption equipment") which performs encryption and a decryption of commo data, for example, a packet, on a communication path.

[0003]

As a procedure of generation of the key used for cryptocommunication in IP network, key exchange, and a key setup, various technique, such as an IKE (Internet Key Exchange: cryptographic key generation procedure) method, exists, for example. A transmitting side enciphers an IP packet using this generated key (cryptographic key), and a receiving side decrypts a packet using the key (decode key) corresponding to this key.

[0004]

By the way, when a certain failure occurs at an optimal path in the midst which is communicating using IP network, a communication link can be recovered, and using the backup routing function which the communication link repeating installation itself, such as a router, has. [using routing protocols such as OSPF (Open Shortest Path First),] That is, an alternate route can be set up automatically and a communication link can be recovered. Hereafter, the outline of these communication link methods of recovery is explained.

[0005]

(1) When a routing protocol is used

As shown in drawing 6, suppose that routers N11-N15 are connected to the node on IP network between a communication device T11 and a communication device 12. The optimal path of forward ' always exchanges mutually the information [information /, i.e., express which router and communication link are directly possible for each router, / the communication device T11 -> router N11

-> router N12 -> router N13 -> router N15 -> communication device T12 or its path formation information / information / which is reverse and has mutually each routers N11-N15], and forms the optimal path between networks.

[0006]

In this optimal path, when a failure occurs in a router N13, the following procedures recover a communication link.

First, the normal router N12 which carries out proximal to a router N13, for example, a router, detects that the failure occurred in the router N13 by the function of a routing protocol. The detection approach is determined by the routing protocol. The router N12 which detected the failure notifies information, such as "an old path was not able to be used" or "the link having been lost", to the adjoining routers N11 and N14 by the function of a routing protocol. Such notice information is relayed also to the adjoining router N15, and, thereby, is notified to all the routers of a routing domain (group of a router who delivers routing information). Thus, the path formation information which each routers N11, N12, N14, and N15 have is updated by the information notified newly, and the reconstitution of the alternate route which becomes instead of a failure path, i.e., the path of the communication device T11 -> router N11 -> router N12 -> router N14 -> router N15 -> communication device T12, is carried out.

[0007]

(2) When a backup routing function is used

A backup routing function is in a certain router N12 in the communication system shown in drawing 6 , for example, a router. the case (polling (supervisory signal) the existence of a link --) where a router N12 detects that the failure occurred for the junction path it is based on keep alive (signal for confirming that the circuit is not downed) etc. -- a router N12 is changed to the alternate route (backup path) set up beforehand based on a backup routing function, and maintains a communication link.

[0008]

[Problem(s) to be Solved by the Invention]

Usually, also when a failure occurs in an optimal path, an alternate route can be formed in the midst which is performing not only a communication link but cryptocommunication using the above-mentioned function and above-mentioned backup routing function of a routing protocol. However, since the function of a routing protocol or the change function to a backup path, and the function of cryptocommunication have another composition, with the existing structure, in the case of cryptocommunication, the enciphered IP packet (encryption data) cannot be decrypted, and it may be unable to continue cryptocommunication. This is explained below.

[0009]

Here, a communication device T11 is connected to the configuration N12 shown in drawing 7 , i.e., a router, through data encryption equipment M21, a communication device T22 is connected to a router N15, and IP network configuration by which data encryption equipment M22 and M23 was connected to juxtaposition between the router N12 and the router N15, respectively is assumed further.

[0010]

Each routers N12 and N15 and data encryption equipment M21 and M22 exchange the path formation information which it has mutually, suit, and form the optimal path between networks. The optimal path in always [forward], i.e., the path at the time of usually converging in a path, is the communication device T11 -> data-encryption-equipment M21 -> router N12 -> data-encryption-equipment M22 -> router N15 -> communication device T12, and data encryption equipment M21 enciphers the packet transmitted from a communication device T22 using the key (for example, the key A) used between self-equipment and data encryption equipment M22.

[0011]

Suppose that a certain failure occurred with data encryption equipment M22, a path change was made by the function of a routing protocol, and the optimal path was automatically changed into the communication device T11 -> data-encryption-equipment M21 -> router N12 -> data-encryption-equipment M23 -> router N15 -> communication device T12 in this condition. In this case, the key (for example, the key B) used between data encryption equipment M21 and data encryption equipment M23

differs from the key A mentioned above. However, in data encryption equipment M21, since there is no modification in the transmission place (communication device T12) of a packet, from the conventional routing protocol, it cannot recognize that the key for codes of the data transmitted to a communication device T12 from a communication device T11 should be changed into Key B from Key A. Therefore, since it will be enciphered with Key A with data encryption equipment M21 and the packet concerned cannot decode this in the data encryption equipment M23 using Key B, cryptocommunication is unrecoverable after all.

[0012]

The tunnel mode which enciphers collectively a part for the data division of IP header which includes the address of a transmission place in cryptocommunication, and a packet (namely, payload), and communicates by attaching IP header including the address of a new transmission place (decryption equipment). Although the transmission place address has the transport mode which does not encipher but enciphers only a part for the data division of a packet, when a failure occurs with data encryption equipment M22 as mentioned above, with data encryption equipment M21, the need for modification of a key can be recognized in neither of the modes.

[0013]

Such a problem is produced in common, the case where a router, data encryption equipment, a communication device, etc. are newly extended by the part (node) which was an optimal path till then, when the parts of a router etc. move, and not only when a path failure occurs during cryptocommunication but when. It originates in having been [this] fixed, and the key used for cryptocommunication having been fixed. [of arrangement of the router in this conventional kind of communication link for Takayoshi etc.]

[0014]

Then, even if this invention is the case where modification arises in the arrangement configuration of the equipment with which the communication link for Takayoshi and cryptocommunication perform encryption and a decryption in a network realizable to coincidence, it makes it a main technical problem to offer the technique which changes the key for codes dynamically and enables it to continue cryptocommunication safely.

[0015]

[Means for Solving the Problem]

The record medium which becomes suitable when a computer realizes the cryptocommunication approach by which this invention was improved in the above-mentioned technical problem for the solution reason, a cryptocommunication system, communication link repeating installation, and communication link repeating installation is offered.

[0016]

The cryptocommunication approach of this invention is an approach of performing communication link for Takayoshi, and cryptocommunication through a network realizable to coincidence. The optimal path on a network is formed by exchanging mutually predetermined path formation information including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible among two or more communication link repeating installation, and suiting on a network. While performing cryptocommunication of commo data between the communication link repeating installation which exists in this optimal path It is characterized by continuing said cryptocommunication using the key fixed mutually between the communication link repeating installation which updates said path formation information, carries out the reconstitution of the new optimal path when the configuration of the communication link repeating installation on said network is changed, and consists in the optimal path by which the reconstitution was carried out and in which cryptocommunication is possible. Each communication link repeating installation records the identification information of the communication device or a network, when a decryption of the enciphered commo data which goes to a certain communication device or network can be performed, and when path formation information is received from other communication link repeating installation and the cryptocommunication point holds the same identification information as said identification

information, it is made to settle between communication link repeating installation besides the above on a key.

[0017]

The cryptocommunication system of this invention is a cryptocommunication system which performs cryptocommunication of commo data between the communication link repeating installation which forms the optimal path on the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence, and exists in this optimal path by exchanging predetermined path formation information mutually among two or more communication link repeating installation, and suiting. The path formation information on each communication link repeating installation is what includes the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible on said network. At least one of two or more of the communication link repeating installation It is constituted so that the arrangement information after the modification concerned may be notified to other communication link repeating installation, when it detects that the arrangement configuration of the communication link repeating installation on the optimal path under cryptocommunication was changed. Other one [at least] While updating the path formation information on self based on said notice and carrying out the reconstitution of the new optimal path to it, it is characterized by being constituted so that said cryptocommunication may be continued using the key fixed mutually between the communication link repeating installation which consists in the optimal path by which the reconstitution was carried out and in which cryptocommunication is possible.

[0018]

In the communication link repeating installation which performs cryptocommunication among other communication link repeating installation which exists in this optimal path while the communication link repeating installation of this invention forms the optimal path of the commo data on a network based on predetermined path formation information Said path formation information is a thing including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible. A means to update the contents of said arrangement information included in the path formation information on self when other communication link repeating installation which serves as a communications partner during cryptocommunication becomes communication link impossible, It is equipment characterized by continuing cryptocommunication using the key which was equipped with a means to form a new optimal path based on the path formation information after updating, and a means to detect other communication link repeating installation in which the cryptocommunication on the newly formed optimal path is possible, and was fixed between the detected communication link repeating installation concerned.

[0019]

it is the information more specifically mutually delivered and carried out among other communication link repeating installation based on a predetermined routing protocol, and, as for path formation information, the information about arrangement of the node which can perform cryptocommunication, and its node fix said key based on this identification information including the identification information of the communication path made into the object of cryptocommunication implementation. When the key fixed between nodes with identification information is held beforehand, the key is ****(ed), and when the key is not held, said key is secured by performing key generation between the nodes concerned.

[0020]

The updating means in communication link repeating installation deletes the arrangement information about it, when the communication link repeating installation used as communication link impossible is during cryptocommunication, when there is communication link repeating installation extended during cryptocommunication, it adds the arrangement information about it, and when there is communication link repeating installation moved during cryptocommunication, it corrects the arrangement information about it.

[0021]

The record medium which this invention offers based on predetermined path formation information

including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible The function which forms the optimal path on the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence, When the function to perform cryptocommunication between communications-partner equipment, and the configuration of said communications-partner equipment are changed, while updating the contents of said arrangement information included in the path formation information on self and forming a new optimal path based on the path formation information after updating It is the record medium with which the program code for forming on a computer the function which continues cryptocommunication using the key fixed among other communications-partner equipments which exist in this new optimal path was recorded and in which a computer readout is possible.

[0022]

[Embodiment of the Invention]

Hereafter, the operation gestalt of this invention is explained with reference to a drawing.

When the communication link for Takayoshi and cryptocommunication are performing cryptocommunication between the equipment which delivers path formation information in a network realizable to coincidence according to a routing protocol, the information about arrangement of the equipment in which cryptocommunication is possible is included in the above-mentioned path formation information, and it is made to make path formation information and the information about modification of a key link in this invention.

For example, if it is the routing protocol of the De Dis wardrobe vector type about between what networks the equipment in which cryptocommunication is possible is arranged to which link, and cryptocommunication can be performed, if it is the routing protocol of a link state type, it will include which router exists in the distance vector into path formation information. And in case encryption data are transmitted, it enables it to perform easily newly generating, if there is no corresponding key using the key corresponding to the data encryption equipment of a reception place.

In addition, use and generation of a key can use the technique generally used from the former.

[0023]

The above-mentioned cryptocommunication approach can be enforced by the cryptocommunication system constituted as shown in drawing 1.

Including the network configuration components of two or more routers L11 which intervene between communication device [of the transmitting side allotted on alpha network] T11, communication device [of the receiving side allotted on beta network] T12, and these communication devices, i.e., A router, D router L12, B router L13, and C router L14, and others, this cryptocommunication system 1 is constituted so that communication link for Takayoshi and cryptocommunication can be realized to coincidence.

It shall connect through a wide area network [like the Internet] whose alpha network and beta network are.

[0024]

Each routers L11-L14 are a kind of computers which have memory and CPU, and have the function of the routing protocol formed by reading the program code with which the CPU was recorded on the predetermined record medium, and performing, the function of cryptocommunication, and the function to make these functions cooperate. Although CPUs are cover-half record media, such as semiconductor memory in which a readout is possible, when mounted in a router, the record medium which recorded this program code circulates through portability record media, such as CD-ROM, and may be installed in the above-mentioned cover-half record medium at the time of mounting.

About the function of a routing protocol, although it is fundamentally [as the thing of the conventional router] the same, it differs from the function with which the router conventional at the point of having made it make the functions of cryptocommunication including the following two information cooperating to the path formation information exchanged for other routers by the routing protocol is equipped.

(1) Arrangement and Interface ID of the node (router) which can perform cryptocommunication

Example: "A router is in A node whose cryptocommunication is possible"

(2) The communication path ID which the node makes the object of cryptocommunication implementation

Example: "the object (communication path ID) of the cryptocommunication in A router receives the communication link of alpha network and gamma network"

The format of the data corresponding to such information becomes what was doubled with the adapted network protocol or the routing protocol. For example, in the case of OSPF of IP network, the information will be included in LSA (Link State Advertisement) mentioned later.

[0025]

On the other hand, about the function of cryptocommunication, as each router is the following, it performs cryptocommunication.

(1) To the communication link corresponding to the communication path ID for cryptocommunication implementation, encipher commo data, for example, a packet, and generate encryption data.

Example: As for the packet to which the source address of the packet which passes A router belongs to gamma network, and the destination address belongs to beta network, it is ****(ed) and used for the key for the codes "which it lets be the objects of cryptocommunication since the destination address suits a communication path ID (2)" when the thing of a node with the communication path ID corresponding to a communication path is held beforehand. When the key is not held, it is performing key generation between the node (router), and a key is secured.

Example: "the router in which cryptocommunication called B router is possible existed on the path addressed to beta network from A router, and A router knows by the routing protocol that the B router is considering as the object of cryptocommunication implementation to beta network. Then, the packet set as the object of cryptocommunication is enciphered using the key corresponding to B router."

About the function to which both function is made to link, it mentions later.

[0026]

In addition, although it is desirable for all the routers L11-L14 to have as for the above function, the operation which has enciphered the packet sent from the communication device T11, and is relayed and which is this invention even if it is the case where only the router which acts mainly has, either is possible.

[0027]

Next, the communication configuration by the cryptocommunication system 1 of this operation gestalt is explained. Here, the communication device T11 in alpha network and the network address between the A routers L11 like illustration "163.135.10.0/24", The interface address between the communication device T12 in beta network, the B router L13, or the C router L14 "163.135.20.0/24", The interface address of the A router L11 "163.135.100.10", The interface address of the B router L13 "163.135.200.20", The example in the case of improving the above OSPF which the network address of the C router L14 shall be "163.135.300.30", and is the representation of a link state type routing protocol, and performing cryptocommunication is given. OSPF is indicated by the specifications RFC2328, RFC1131, and STD0054 published in the international organization IETF at the detail.

[0028]

The example of a format of the router link LSA which each routers L11-L14 transmit among the path formation information used by OSPF, i.e., a link condition advertising packet, (LSA:Link State Advertisement) is shown in drawing 2.

This router link LSA is various link informations received and passed between proximal routers, and consists of a link condition header and a LSA section. Using the information which a router type, Link ID, link data, etc. are described by the LSA section, and is described by this, each router can recognize the information about arrangement of other routers, and can use now for path computation or a recalculation. Drawing 3 shows the router type contents and the example of the Link ID and link data to it. Types 1-4 are information which the existing router possesses, and Type 5 is the part added with this operation gestalt, i.e., the information relevant to cryptocommunication. By this type 5 of description, which router understands where cryptocommunication is performed. In Type 5, when link data are Null,

it is shown that somewhere which is not determined yet and cryptocommunication can be performed.
[0029]

LSA can send two or more link informations which it can have with each routers L11-L14. Therefore, if one router is performing cryptocommunication among two or more routers, two or more LSA(s) for cryptocommunication can also be specified. For example, it is shown that the router which has as the address "163.135.100.10" which transmitted this LSA by LSA of Type 5 if Link ID is "163.135.100.10" and link data are "163.135.20.0/24" is in the condition which can perform a phase hand with the address of "163.135.20.0/24" and cryptocommunication. Furthermore, it is the same to Link ID, and if there is LSA of link data "163.135.30.0/24", it is shown that a router "163.135.100.10" is in the condition whose cryptocommunication is possible also with "163.135.30.0/24" of phase hands.

[0030]

Such amelioration OSPF is used, and when enciphering a packet and transmitting, each routers L11-L14 will declare the information on the cryptocommunication point by LSA. The information on cryptocommunication origin is also included in this declaration. Each routers L11-L14 record the information on the network on the own database of a router as "a cryptocommunication charge network (or host)", when a decryption of the packet which goes to a certain network can be performed again. This information turns into information required in order to perform key generation between that LSA transmitting former routers, when each router receives the cryptocommunication LSA of other routers and it has the same "cryptocommunication charge network" as that cryptocommunication point.

[0031]

Routers are delivering the Hello packet (a thing like a keep alive signal to a contiguity router), respectively, and self LSA gets across to the other party by the link-Bayh-link between the routers in which this delivery is possible, respectively. For example, when the B router L13 and the C router L14 are routers in which encryption and a decryption are possible, that that and it are operating normally gets across to the A router L11 through the D router L12. The A router L11 gets to know that it is ready for the router L13 to perform self "cryptocommunication charge network" and cryptocommunication by LSA of the B router L13, and carries out the process which generates the key for codes between the B routers L13. This process may be a process of key generation of generally being used. The A router L11 carries out the process which generates a key also between the C routers L14 again.

[0032]

Drawing 4 (a) is drawing having shown the contents of the link table (former information on routing table) of the A router L11 when usually converging in a path. In the example of illustration, the A router L11 is linked with alpha network and the D router L12, and cryptocommunication charge networks are alpha and gamma. The B router L13 and the C router L14 are linked with beta network and the D router L12, and both "cryptocommunication charge networks" is beta. Or it links D router with the A router L11, the B router L13, and the C router L14 and it does not have assignment of a "cryptocommunication charge network", it is somewhere which is not yet determined. In addition, the "cryptocommunication charge network" does not necessarily need to adjoin.

[0033]

This link table to the A router L11 forms the optimal path to Network beta from Network alpha like an alpha network (communication device T11) ->A router L11 ->D router L12 ->B router L13 ->beta network (communication device T12).

[0034]

On the other hand, the A router L11 cooperates with the link table of drawing 4 (a), and sets up an encryption filter like drawing 5 (a). That is, the "cryptocommunication charge network" of the A router L11 is an alpha network, and the router which makes beta a "cryptocommunication charge network" on a path is the B router L13. Then, the A router L11 generates Key a between the B routers L13 (it is **** (ed) when Key a is already held). The semantics of this link table is "the sending agency address's (network's) being alpha, and the transmission place address's (network's) enciphering the packet (alpha->beta) of beta with Key a, and transmitting to the B router L13 (set peer (B))." Thereby, the cryptocommunication using Key a becomes possible.

[0035]

Here, the case where a failure occurs in the B router L13 is considered.

In this case, since LSA which the B router L13 emits does not reach the D router L12 and the A router L11, the A router L11 recovers a path as what cannot use the B router L13 using the function of a routing protocol. Drawing 4 (b) is drawing having shown the contents after renewal of the link table (origin of routing table) of the A router L11 when converging in a recovery path. Like illustration, the link information of the B router L13 is lost. Although an optimal path is changed from this link table like an alpha network (communication device T11) ->A router L11 ->D router L12 ->C router L14 ->beta network (communication device T12), the key a which cooperates with path modification and the A router L11 uses further is made to change into Key c dynamically with this operation gestalt.

[0036]

That is, if the link table of drawing 4 (b) is updated, the A router L11 will cooperate to this, and will update the contents of the encryption filter like drawing 5 (b). That is, since, as for the router which makes beta a "cryptocommunication charge network" on a path, it turns out that it is the C router L14, the A router L11 generates Key c between the C routers L14 (it is ****(ed) when Key c is already held). The semantics of this link table is "the sending agency address's (network's) being alpha, and the transmission place address's (network's) enciphering the packet (alpha->beta) of beta with Key c, and transmitting to the C router L14 (set peer (B))."

[0037]

Thus, since a setup of an encryption filter like drawing 5 (b) is obtained from the link table by the routing protocol after updating and modification of the key accompanying path modification is made even if a failure occurs in the B router L13 and path modification is made, cryptocommunication can be continued.

[0038]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]

Usually, also when a failure occurs in an optimal path, an alternate route can be formed in the midst which is performing not only a communication link but cryptocommunication using the above-mentioned function and above-mentioned backup routing function of a routing protocol. However, since the function of a routing protocol or the change function to a backup path, and the function of cryptocommunication have another composition, with the existing structure, in the case of cryptocommunication, the enciphered IP packet (encryption data) cannot be decrypted, and it may be unable to continue cryptocommunication. This is explained below.

[0009]

Here, a communication device T11 is connected to the configuration N12 shown in drawing 7, i.e., a router, through data encryption equipment M21, a communication device T22 is connected to a router N15, and IP network configuration by which data encryption equipment M22 and M23 was connected to juxtaposition between the router N12 and the router N15, respectively is assumed further.

[0010]

Each routers N12 and N15 and data encryption equipment M21 and M22 exchange the path formation information which it has mutually, suit, and form the optimal path between networks. The optimal path in always [forward], i.e., the path at the time of usually converging in a path, is the communication device T11 -> data-encryption-equipment M21 -> router N12 -> data-encryption-equipment M22 -> router N15 -> communication device T12, and data encryption equipment M21 enciphers the packet transmitted from a communication device T22 using the key (for example, the key A) used between self-equipment and data encryption equipment M22.

[0011]

Suppose that a certain failure occurred with data encryption equipment M22, a path change was made by the function of a routing protocol, and the optimal path was automatically changed into the communication device T11 -> data-encryption-equipment M21 -> router N12 -> data-encryption-equipment M23 -> router N15 -> communication device T12 in this condition. In this case, the key (for example, the key B) used between data encryption equipment M21 and data encryption equipment M23 differs from the key A mentioned above. However, in data encryption equipment M21, since there is no modification in the transmission place (communication device T12) of a packet, from the conventional routing protocol, it cannot recognize that the key for codes of the data transmitted to a communication device T12 from a communication device T11 should be changed into Key B from Key A. Therefore, since it will be enciphered with Key A with data encryption equipment M21 and the packet concerned cannot decode this in the data encryption equipment M23 using Key B, cryptocommunication is unrecoverable after all.

[0012]

The tunnel mode which enciphers collectively a part for the data division of IP header which includes the address of a transmission place in cryptocommunication, and a packet (namely, payload), and communicates by attaching IP header including the address of a new transmission place (decryption

equipment), Although the transmission place address has the transport mode which does not encipher but enciphers only a part for the data division of a packet, when a failure occurs with data encryption equipment M22 as mentioned above, with data encryption equipment M21, the need for modification of a key can be recognized in neither of the modes.

[0013]

Such a problem is produced in common, the case where a router, data encryption equipment, a communication device, etc. are newly extended by the part (node) which was an optimal path till then, when the parts of a router etc. move, and not only when a path failure occurs during cryptocommunication but when. It originates in having been [this] fixed, and the key used for cryptocommunication having been fixed. [of arrangement of the router in this conventional kind of communication link for Takayoshi etc.]

[0014]

Then, even if this invention is the case where modification arises in the arrangement configuration of the equipment with which the communication link for Takayoshi and cryptocommunication perform encryption and a decryption in a network realizable to coincidence, it makes it a main technical problem to offer the technique which changes the key for codes dynamically and enables it to continue cryptocommunication safely.

[0015]

[Translation done.]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem]

The record medium which becomes suitable when a computer realizes the cryptocommunication approach by which this invention was improved in the above-mentioned technical problem for the solution reason, a cryptocommunication system, communication link repeating installation, and communication link repeating installation is offered.

[0016]

The cryptocommunication approach of this invention is an approach of performing communication link for Takayoshi, and cryptocommunication through a network realizable to coincidence. The optimal path on a network is formed by exchanging mutually predetermined path formation information including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible among two or more communication link repeating installation, and suiting on a network. While performing cryptocommunication of commo data between the communication link repeating installation which exists in this optimal path It is characterized by continuing said cryptocommunication using the key fixed mutually between the communication link repeating installation which updates said path formation information, carries out the reconstitution of the new optimal path when the configuration of the communication link repeating installation on said network is changed, and consists in the optimal path by which the reconstitution was carried out and in which cryptocommunication is possible. Each communication link repeating installation records the identification information of the communication device or a network, when a decryption of the enciphered commo data which goes to a certain communication device or network can be performed, and when path formation information is received from other communication link repeating installation and the cryptocommunication point holds the same identification information as said identification information, it is made to settle between communication link repeating installation besides the above on a key.

[0017]

The cryptocommunication system of this invention is a cryptocommunication system which performs cryptocommunication of commo data between the communication link repeating installation which forms the optimal path on the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence, and exists in this optimal path by exchanging predetermined path formation information mutually among two or more communication link repeating installation, and suiting. The path formation information on each communication link repeating installation is what includes the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible on said network. At least one of two or more of the communication link repeating installation It is constituted so that the arrangement information after the modification concerned may be notified to other communication link repeating installation, when it detects that the arrangement configuration of the communication link repeating installation on the optimal path under cryptocommunication was changed. Other one [at least] While updating the path formation information on self based on said notice and carrying out the reconstitution of the new

optimal path to it, it is characterized by being constituted so that said cryptocommunication may be continued using the key fixed mutually between the communication link repeating installation which consists in the optimal path by which the reconstitution was carried out and in which cryptocommunication is possible.

[0018]

In the communication link repeating installation which performs cryptocommunication among other communication link repeating installation which exists in this optimal path while the communication link repeating installation of this invention forms the optimal path of the commo data on a network based on predetermined path formation information Said path formation information is a thing including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible. A means to update the contents of said arrangement information included in the path formation information on self when other communication link repeating installation which serves as a communications partner during cryptocommunication becomes communication link impossible, It is equipment characterized by continuing cryptocommunication using the key which was equipped with a means to form a new optimal path based on the path formation information after updating, and a means to detect other communication link repeating installation in which the cryptocommunication on the newly formed optimal path is possible, and was fixed between the detected communication link repeating installation concerned.

[0019]

it is the information more specifically mutually delivered and carried out among other communication link repeating installation based on a predetermined routing protocol, and, as for path formation information, the information about arrangement of the node which can perform cryptocommunication, and its node fix said key based on this identification information including the identification information of the communication path made into the object of cryptocommunication implementation. When the key fixed between nodes with identification information is held beforehand, the key is ****(ed), and when the key is not held, said key is secured by performing key generation between the nodes concerned.

[0020]

The updating means in communication link repeating installation deletes the arrangement information about it, when the communication link repeating installation used as communication link impossible is during cryptocommunication, when there is communication link repeating installation extended during cryptocommunication, it adds the arrangement information about it, and when there is communication link repeating installation moved during cryptocommunication, it corrects the arrangement information about it.

[0021]

The record medium which this invention offers based on predetermined path formation information including the arrangement information about arrangement of the communication link repeating installation in which cryptocommunication is possible The function which forms the optimal path on the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence, When the function to perform cryptocommunication between communications-partner equipment, and the configuration of said communications-partner equipment are changed, while updating the contents of said arrangement information included in the path formation information on self and forming a new optimal path based on the path formation information after updating It is the record medium with which the program code for forming on a computer the function which continues cryptocommunication using the key fixed among other communications-partner equipments which exist in this new optimal path was recorded and in which a computer readout is possible.

[0022]

[Embodiment of the Invention]

Hereafter, the operation gestalt of this invention is explained with reference to a drawing.

When the communication link for Takayoshi and cryptocommunication are performing cryptocommunication between the equipment which delivers path formation information in a network realizable to coincidence according to a routing protocol, the information about arrangement of the

equipment in which cryptocommunication is possible is included in the above-mentioned path formation information, and it is made to make path formation information and the information about modification of a key link in this invention.

For example, if it is the routing protocol of the De Dis wardrobe vector type about between what networks the equipment in which cryptocommunication is possible is arranged to which link, and cryptocommunication can be performed, if it is the routing protocol of a link state type, it will include which router exists in the distance vector into path formation information. And in case encryption data are transmitted, it enables it to perform easily newly generating, if there is no corresponding key using the key corresponding to the data encryption equipment of a reception place.

In addition, use and generation of a key can use the technique generally used from the former.

[0023]

The above-mentioned cryptocommunication approach can be enforced by the cryptocommunication system constituted as shown in drawing 1.

Including the network configuration components of two or more routers L11 which intervene between communication device [of the transmitting side allotted on alpha network] T11, communication device [of the receiving side allotted on beta network] T12, and these communication devices, i.e., A router, D router L12, B router L13, and C router L14, and others, this cryptocommunication system 1 is constituted so that communication link for Takayoshi and cryptocommunication can be realized to coincidence.

It shall connect through a wide area network [like the Internet] whose alpha network and beta network are.

[0024]

Each routers L11-L14 are a kind of computers which have memory and CPU, and have the function of the routing protocol formed by reading the program code with which the CPU was recorded on the predetermined record medium, and performing, the function of cryptocommunication, and the function to make these functions cooperate. Although CPUs are cover-half record media, such as semiconductor memory in which a readout is possible, when mounted in a router, the record medium which recorded this program code circulates through portability record media, such as CD-ROM, and may be installed in the above-mentioned cover-half record medium at the time of mounting.

About the function of a routing protocol, although it is fundamentally [as the thing of the conventional router] the same, it differs from the function with which the router conventional at the point of having made it make the functions of cryptocommunication including the following two information cooperating to the path formation information exchanged for other routers by the routing protocol is equipped.

(1) Arrangement and Interface ID of the node (router) which can perform cryptocommunication

Example: "A router is in A node whose cryptocommunication is possible"

(2) The communication path ID which the node makes the object of cryptocommunication implementation

Example: "the object (communication path ID) of the cryptocommunication in A router receives the communication link of alpha network and gamma network"

The format of the data corresponding to such information becomes what was doubled with the adapted network protocol or the routing protocol. For example, in the case of OSPF of IP network, the information will be included in LSA (Link State Advertisement) mentioned later.

[0025]

On the other hand, about the function of cryptocommunication, as each router is the following, it performs cryptocommunication.

(1) To the communication link corresponding to the communication path ID for cryptocommunication implementation, encipher commo data, for example, a packet, and generate encryption data.

Example: As for the packet to which the source address of the packet which passes A router belongs to gamma network, and the destination address belongs to beta network, it is ****(ed) and used for the key for the codes "which it lets be the objects of cryptocommunication since the destination address suits a

communication path ID (2)" when the thing of a node with the communication path ID corresponding to a communication path is held beforehand. When the key is not held, it is performing key generation between the node (router), and a key is secured.

Example: "the router in which cryptocommunication called B router is possible existed on the path addressed to beta network from A router, and A router knows by the routing protocol that the B router is considering as the object of cryptocommunication implementation to beta network. Then, the packet set as the object of cryptocommunication is enciphered using the key corresponding to B router."

About the function to which both function is made to link, it mentions later.

[0026]

In addition, although it is desirable for all the routers L11-L14 to have as for the above function, the operation which has enciphered the packet sent from the communication device T11, and is relayed and which is this invention even if it is the case where only the router which acts mainly has, either is possible.

[0027]

Next, the communication configuration by the cryptocommunication system 1 of this operation gestalt is explained. Here, the communication device T11 in alpha network and the network address between the A routers L11 like illustration "163.135.10.0/24", The interface address between the communication device T12 in beta network, the B router L13, or the C router L14 "163.135.20.0/24", The interface address of the A router L11 "163.135.100.10", The interface address of the B router L13 "163.135.200.20", The example in the case of improving the above OSPF which the network address of the C router L14 shall be "163.135.300.30", and is the representation of a link state type routing protocol, and performing cryptocommunication is given. OSPF is indicated by the specifications RFC2328, RFC1131, and STD0054 published in the international organization IETF at the detail.

[0028]

The example of a format of the router link LSA which each routers L11-L14 transmit among the path formation information used by OSPF, i.e., a link condition advertising packet, (LSA:Link State Advertisement) is shown in drawing 2.

This router link LSA is various link informations received and passed between proximal routers, and consists of a link condition header and a LSA section. Using the information which a router type, Link ID, link data, etc. are described by the LSA section, and is described by this, each router can recognize the information about arrangement of other routers, and can use now for path computation or a re-calculation. Drawing 3 shows the router type contents and the example of the Link ID and link data to it. Types 1-4 are information which the existing router possesses, and Type 5 is the part added with this operation gestalt, i.e., the information relevant to cryptocommunication. By this type 5 of description, which router understands where cryptocommunication is performed. In Type 5, when link data are Null, it is shown that somewhere which is not determined yet and cryptocommunication can be performed.

[0029]

LSA can send two or more link informations which it can have with each routers L11-L14. Therefore, if one router is performing cryptocommunication among two or more routers, two or more LSA(s) for cryptocommunication can also be specified. For example, it is shown that the router which has as the address "163.135.100.10" which transmitted this LSA by LSA of Type 5 if Link ID is "163.135.100.10" and link data are "163.135.20.0/24" is in the condition which can perform a phase hand with the address of "163.135.20.0/24" and cryptocommunication. Furthermore, it is the same to Link ID, and if there is LSA of link data "163.135.30.0/24", it is shown that a router "163.135.100.10" is in the condition whose cryptocommunication is possible also with "163.135.30.0/24" of phase hands.

[0030]

Such amelioration OSPF is used, and when enciphering a packet and transmitting, each routers L11-L14 will declare the information on the cryptocommunication point by LSA. The information on cryptocommunication origin is also included in this declaration. Each routers L11-L14 record the information on the network on the own database of a router as "a cryptocommunication charge network (or host)", when a decryption of the packet which goes to a certain network can be performed again.

This information turns into information required in order to perform key generation between that LSA transmitting former routers, when each router receives the cryptocommunication LSA of other routers and it has the same "cryptocommunication charge network" as that cryptocommunication point.

[0031]

Routers are delivering the Hello packet (a thing like a keep alive signal to a contiguity router), respectively, and self LSA gets across to the other party by the link-Bayh-link between the routers in which this delivery is possible, respectively. For example, when the B router L13 and the C router L14 are routers in which encryption and a decryption are possible, that that and it are operating normally gets across to the A router L11 through the D router L12. The A router L11 gets to know that it is ready for the router L13 to perform self "cryptocommunication charge network" and cryptocommunication by LSA of the B router L13, and carries out the process which generates the key for codes between the B routers L13. This process may be a process of key generation of generally being used. The A router L11 carries out the process which generates a key also between the C routers L14 again.

[0032]

Drawing 4 (a) is drawing having shown the contents of the link table (former information on routing table) of the A router L11 when usually converging in a path. In the example of illustration, the A router L11 is linked with alpha network and the D router L12, and cryptocommunication charge networks are alpha and gamma. The B router L13 and the C router L14 are linked with beta network and the D router L12, and both "cryptocommunication charge networks" is beta. Or it links D router with the A router L11, the B router L13, and the C router L14 and it does not have assignment of a "cryptocommunication charge network", it is somewhere which is not yet determined. In addition, the "cryptocommunication charge network" does not necessarily need to adjoin.

[0033]

This link table to the A router L11 forms the optimal path to Network beta from Network alpha like an alpha network (communication device T11) ->A router L11 ->D router L12 ->B router L13 ->beta network (communication device T12).

[0034]

On the other hand, the A router L11 cooperates with the link table of drawing 4 (a), and sets up an encryption filter like drawing 5 (a). That is, the "cryptocommunication charge network" of the A router L11 is an alpha network, and the router which makes beta a "cryptocommunication charge network" on a path is the B router L13. Then, the A router L11 generates Key a between the B routers L13 (it is ****(ed) when Key a is already held). The semantics of this link table is "the sending agency address's (network's) being alpha, and the transmission place address's (network's) enciphering the packet (alpha->beta) of beta with Key a, and transmitting to the B router L13 (set peer (B))." Thereby, the cryptocommunication using Key a becomes possible.

[0035]

Here, the case where a failure occurs in the B router L13 is considered.

In this case, since LSA which the B router L13 emits does not reach the D router L12 and the A router L11, the A router L11 recovers a path as what cannot use the B router L13 using the function of a routing protocol. Drawing 4 (b) is drawing having shown the contents after renewal of the link table (origin of routing table) of the A router L11 when converging in a recovery path. Like illustration, the link information of the B router L13 is lost. Although an optimal path is changed from this link table like an alpha network (communication device T11) ->A router L11 ->D router L12 ->C router L14 ->beta network (communication device T12), the key a which cooperates with path modification and the A router L11 uses further is made to change into Key c dynamically with this operation gestalt.

[0036]

That is, if the link table of drawing 4 (b) is updated, the A router L11 will cooperate to this, and will update the contents of the encryption filter like drawing 5 (b). That is, since, as for the router which makes beta a "cryptocommunication charge network" on a path, it turns out that it is the C router L14, the A router L11 generates Key c between the C routers L14 (it is ****(ed) when Key c is already held). The semantics of this link table is "the sending agency address's (network's) being alpha, and the

transmission place address's (network's) enciphering the packet (alpha->beta) of beta with Key c, and transmitting to the C router L14 (set peer (B))."

[0037]

Thus, since a setup of an encryption filter like drawing 5 (b) is obtained from the link table by the routing protocol after updating and modification of the key accompanying path modification is made even if a failure occurs in the B router L13 and path modification is made, cryptocommunication can be continued.

[0038]

In addition, although it assumed that modification arose in the arrangement configuration of the router in which cryptocommunication is possible, and the path failure by failure of a router etc. arose as an example in case the key used by this is changed with this operation gestalt This invention can be similarly applied, not only an example such but when the key to be used is changed, as a result of extending a router for example, on a network or moving a router to other networks from a certain network. That is, it is possible to continue cryptocommunication by delivering path formation information mutually using the function of a routing protocol, updating the arrangement information with each router, and forming an optimal path automatically, without setting up cryptocommunication by hand control. Moreover, the router concerned becomes possible [also finding out the phase hand equipment which performs cryptocommunication automatically] only by specifying the target network thru/or target host who performs cryptocommunication as the path formation information on a router. These functions are functions adapted to the actual communication configuration that the number of the routers connected on a certain network fluctuates continuously, and correspondence becomes possible easily by this also at the spread of mobile mold communication links.

[0039]

Although the router was mentioned as the example and this operation gestalt explained it as communication link repeating installation, the structure of this invention can be applied to the equipment at large which is in case the phase hand of cryptocommunication changes. Moreover, although it is a desirable gestalt to prepare the function to deliver path formation information to other equipments and mutual like this operation gestalt, and the function to make the key for codes change dynamically, in one equipment (for example, router), it is not having to make it such [always] a gestalt. For example, it does not become trouble to constitute so that the communication device connected to the router may have the function to change the key for codes dynamically based on the notice from a router, when enforcing the cryptocommunication approach of this invention.

[0040]

although this operation gestalt explained the example which made IP network communication media, if this invention is the network which can realize communication link for Takayoshi, and cryptocommunication to coincidence, since it is applicable irrespective of the scale -- ANSE -- use with the intranet and extranet which are a cure network is also possible.

[0041]

Since the mutual delivery function of path formation information like a routing protocol becomes application of this invention with a premise, Although it will use within the closed network which does not use the ISP when using other original routing protocols or using ISP (Internet Service Provider) which cannot perform interconnect of a routing protocol Even if it is the case where the ISP is used, use in the network beyond a closed network is also possible by relaying path formation information by the approach by service of ISP with a well-known tunneling technique.

[0042]

It can respond also to a network configuration change which are effective especially when it is changed frequently logically, and is called a mobile network physically [this invention / the cryptocommunication point] flexibly.

[0043]

Application in the cryptocommunication commercial scene for consumer (one gestalt of use of the network service for an individual) is also possible for this invention again. The mainstream of the

cryptocommunication technique for current and an individual is SSL (Secure Socket Layer). This aims at performing cryptocommunication of end to end by enciphering by the communicative upper layer, and the terminal (communication device) itself which an individual operates enciphering commo data, and transmitting. It can become an effective means to make this invention apply to the network which the terminal (a mobile mold terminal is included) which this individual operates accesses, when promoting the above-mentioned network service.
[0044]

[Translation done.]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The cryptocommunication structure-of-a-system Fig. which applied this invention.

[Drawing 2] Drawing having shown the example of a format of the router link LSA.

[Drawing 3] Drawing having shown the type class of router link LSA.

[Drawing 4] For (a), (b) is the contents explanatory view of the link table used when forming the optimal path at the time of using a routing protocol, and the contents explanatory view of the link table updated at the time of failure generating.

[Drawing 5] For (a), (b) is drawing having shown the contents of a setting of the encryption filter at the time of normal actuation, and drawing having shown the contents of a setting of the encryption filter updated at the time of failure generating.

[Drawing 6] The network configuration Fig. for using for the explanation of the optimal-path restoration at the time of using a routing protocol in the former.

[Drawing 7] It is a network configuration Fig. for using for explanation of the optimal-path restoration at the time of using the routing protocol and cryptocommunication in the former.

[Description of Notations]

1 Cryptocommunication System

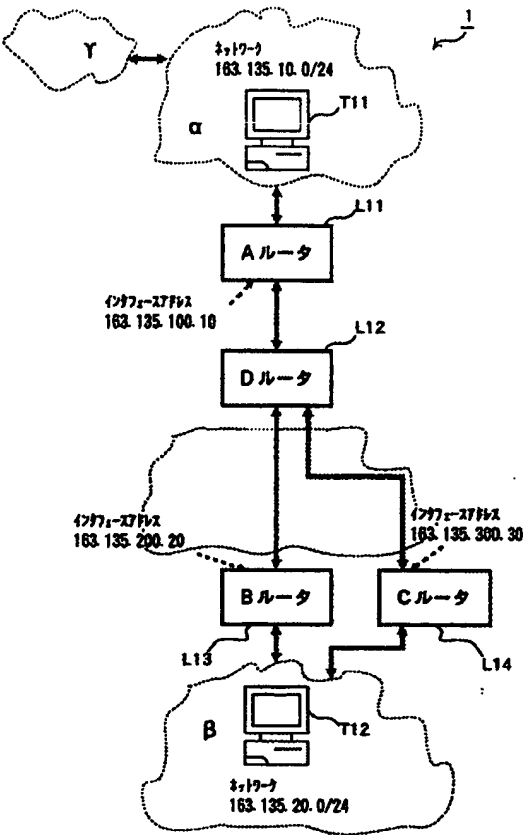
T11, T12 Communication device

L11-L14, N11-N15 Router

M21-M23 Data encryption equipment

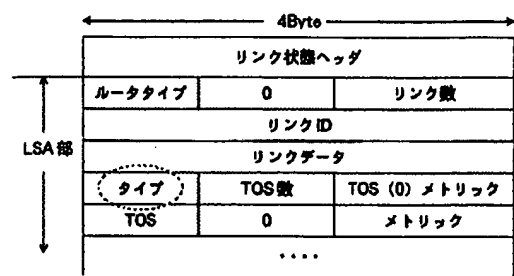
[Translation done.]

Drawing selection | drawing 1



[Translation done.]

Drawing selection drawing 2



[Translation done.]


| タイプ | 内容 | リンク ID | リンクデータ |
|---------------|---------------------------|--|--|
| 1 | 他のルータへのポイント・ツー・ポイントコネクション | 隣接ルータのルータ ID | インタフェース番号 (または IP アドレス) |
| 2 | 通過ネットワークへのコネクション | 代表ルータへのアドレス | ルータのそのネットワーク上の IP アドレス |
| 3 | スタブ・ネットワークへのコネクション | そのネットワークに対する、アドレスプレフィクス | プレフィクス長 |
| 4 | 仮想リンク | 隣接ルータのルータ ID | ルータのそのネットワーク上の IP アドレス |
| 5 (追加する部分) | 暗号通信 | 暗号通信ができる 自ノードの IP アドレスか ルータ ID、 またはインタフェース番号、 またはインタフェースの IP アドレス | 暗号通信ができる 相手先の ネットワークアドレス またはホストアドレス |

(a)

| ルータ | A | B | C | D |
|--------------------|-----------------------|----------------------|----------------------|-------------------------|
| 持っているリンク (コスト) | α (1) D (1) | β (1) D (1) | β (1) D (2) | A (1) B (1) C (2) |
| 暗号通信受け待ち ネットワーク | α γ | β | β | N/A |

(b)

| ルータ | A | C | D |
|--------------------|-----------------------|----------------------|-------------------------|
| 持っているリンク (コスト) | α (1) D (1) | β (1) D (2) | A (1) B (1) C (2) |
| 暗号通信受け待ち ネットワーク | α γ | β | N/A |

Drawing selection | drawing 5 

(a)

| | |
|----------|----------------------------|
| match | $\alpha \rightarrow \beta$ |
| set peer | (B) |
| key | a |

(b)

| | |
|----------|----------------------------|
| match | $\alpha \rightarrow \beta$ |
| set peer | (C) |
| key | c |

[Translation done.]

